Survival Guide

netwrix
#1 for change auditing

ShellShock Survival Guide

Quick Survival Guide About ShellShock Vulnerability

1. Quick Description

- ShellShock breach (aka Bashdoor) is a security bug in the Unix Bash shell.

2. When Discovered

- 24 September 2014

3. What Bash Versions Affected

- Everything through 4.3

4. What Systems Affected

- All Unix based systems (Apache, Cisco iOS etc…), Linux and Mac OS X operation systems.

5. Threat (Very High!)

- Allows an attacker to cause Bash to execute arbitrary commands, allowing an attacker to gain unauthorized access to a computer system, which can lead to dumping internal files for public retrieval if we speak about Apache based Internet sites. In addition, password and configuration files with credentials leakage, extending to any other files access/leakage on the system.
- The same approach can be applied to write files to the system. This is a very easy way of distributing malware.
- **Moreover, ShellShock execution via CGI scripts does not require any authentication at all!**

6. How to Discover Vulnerability

□ Run the following command in your bash shell:

```
env X="() { :;} ; echo busted" /bin/sh -c "echo stuff"
env X="() { :;} ; echo busted" 'which bash' -c "echo completed"
```

□ If you get “busted” echo’d back out, then your systems can be exploited by ShellShock.

7. How Protect Your IT Infrastructure

□ Patching at risk systems: Red Hat, Cisco, HP, UBUNTU, DEBIAN, VMware, CentOS, Novell/SUSE and others.

□ Update your IPS/IDS definitions/digital vaccines!

□ Optional (**not recommended, because that could have tangible business impact**) - Replace Bash with an alternate shell implementation or turn off at-risk systems.